DOI 10.52363/2414-5866-2024-2-11
УДК 355/359.07; 342.08

Галушко С.П., *Центр пункту управління Головного командного центру, м. Киев*
ORCID: 0009-0005-3169-1478

Galushko S., *Command Post Center of the Main Command Center, Kyiv*

МОДЕЛЬ ФУНКЦІОНУВАННЯ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ ТА ВПЛИВУ ЇЇ ТЕХНОЛОГІЙ

THE FUNCTIONAL MODEL OF PUBLIC ADMINISTRATION MECHANISMS IN THE SPHERE OF NATIONAL SECURITY IN THE CONDITIONS OF DIGITALIZATION AND THE INFLUENCE OF ITS TECHNOLOGIES

Досліджено теоретичні засади формування й оцінювання моделі публічного управління у сфері національної безпеки в умовах цифровізації. Обґрунтовано роль технологій штучного інтелекту у сфері забезпечення у сфері національної безпеки.

Ключові слова: *публічне управління, сфера національної безпеки, цифровізація, технології цифровізації, цифрова трансформація, органи влади.*

The theoretical principles of public administration in the field of national security in the conditions of digitalization have been studied. The role of artificial intelligence in the provision of national security is substantiated.

Keywords: *public administration, sphere of national security, digitalization, digitalization technologies, digital transformation, authorities.*

Постановка проблеми. Неоголошена ві йна рф проти України є різновидом гібридної війни, що передбачає використання класичної кінетичної зброї та нетрадиційної зброї. Остання здебільшого є новітньою та оновлюється так само стрімко, як і з’являється. Особливу загрозу становить «комбо» зброя, що охоплює використання цифрових технологій для застосування кінетичної зброї та нетрадиційної. Вітчизняні та закордонні дослідники слушно звертають увагу на ці аспекти, намагаючись спрогнозувати вплив цифрових технологій на національну безпеку. Адже

технології, пов’язані зі штучним інтелектом, змінюють звичний порядок життя, у т.ч. впливають на рівень внутрішньої та міжнародної (глобальної) безпеки. Крім того, ці технології забезпечують трансформацію системи публічного управління у сфері забезпечення національної безпеки. Зважаючи на викладене, можемо визнати важливість науково-теоретичного дослідження особливостей впливу цифрових технологій на сферу національної безпеки.

Аналіз останніх досліджень і публікацій. Концептуальні засади формування та реалізації державної політики у сфері забезпечення національної безпеки й оцінювання впливу факторів на цю сферу визначені в публікаціях Базилюк Я., Гриценко А., Денисенко М., Джохансона Ф., Домбровської С., Ємангова В., Карсруда А., Клюта Р., Колісніченко П., Крюкова О., Кумара С., Лекаря С., Наєма Х., Нижник Н., Помази-Пономаренко А., Почепцова Г, Ситника Г., Тайера А., Чуба С., Щепанського Е. та інших [1; 2–4; 5; 8; 10]. У той же час, низка питань щодо оцінювання моделі реалізації державної політики у сфері забезпечення національної безпеки в умовах впливу цифрових технологій залишаються недостатньо дослідженими, і ці аспекти пов’язані з використанням новітніх технологій.

Постановка завдання. Метою статті є обґрунтування моделі функціонування механізмів публічного управління у сфері національної безпеки в умовах цифровізації та впливу її технологій.

Виклад основного матеріалу. Група вчених слушно зауважили, що підвищення рівня національної безпеки вимагає прийняття дієвих управлінських рішень, що ґрунтується на певній інформації [1; 2–4; 5; 9; 12]. З огляду на це набуває актуальності питання використання, обміну, аналізу інформації, а також забезпечення оперативності, комплексності та виваженості в застосуванні підходів до оцінювання механізмів державного управління. Даний процес відноситься до реалізації контрольної функції, що охоплює, як відомо, моніторинг, аналіз і коригування.

Збільшення джерел даних, їх варіативність, поширеність й обсяги нарівні з підвищенням обчислювальних потужностей зумовлюють стрімкий розвиток різних технологічних концепцій, де метадані виступають своєрідним базисом. Це призводить до появи нової соціально-політичної моделі «цифровізації», що, з одного боку, забезпечує модернізацію приватного й державного секторів, а з іншого – ці сектори стають мішенню, площадкою для апробації цифрових технології з метою дестабілізації нормальної роботи цих секторів.

На механізм оцінювання стану реалізації публічного управління у сфері національної безпеки в умовах розвитку технологій цифровізації можуть впливати зовнішні та внутрішні фактори. Вони вимагають створення необхідних умов, за яких відбуватиметься результативне протистояння негативному впливу цих цифрових технологій (рис. 1).

При цьому оцінювання факторів, що впливають на стан національної безпеки, має відбуватись у межах чітко окресленого алгоритму (порядку) (рис. 2).

Рис. 2.3. Умови застосування механізмів протистояння загрозам, пов’язаним із використанням цифрових технологій

Джерело: складено на підставі [1, с. 120, 134–135; 2–4; 5; 9; 12]

Слід зауважити, що розрахунок загроз у сфері підтримання національної безпеки в умовах впливу цифровізації може мати такий вигляд:

$$TE = \frac{(PV \cdot (TP + TT))}{(DA \cdot TF)} \qquad (1)$$

Формула розрахунку загроз містить показники значущості (PV), сприйняття загроз (TP), показник характеру/типу загрози (TT), показник кількості об’єктів (DA), що захищаються, і показник факторів загроз (TF).

Іншими словами, логічний зміст формули можна представити таким чином: оцінка загроз (ТЕ) є відношенням суми показника сприйняття загроз (ТР – як загрози представлені на рівні нормативно-правових актів) та показника характеру/типу загрози (ТТ – як загрози представлені у звітах, релевантній літературі) помножена на показник значущості (PV – як особи, яка приймає рішення та політичні актори, які оцінюють важливість/значимість загроз) до показника кількості об'єктів, що захищаються (DA – об'єкти/активи на які спрямовані загрози) на показник факторів загроз (TF – оцінка та ранжування секторів безпеки до яких відносяться загрози).

Відмінна ознака формули (1) – це те, що уряди повинні враховувати та співвідносити загрози з тим, на яку складову нацбезпеки останні спрямовані (на соціальну сферу, освітню, наукову, економічну, екологічну тощо). Детальний опис розрахунку формули представлений нижче.

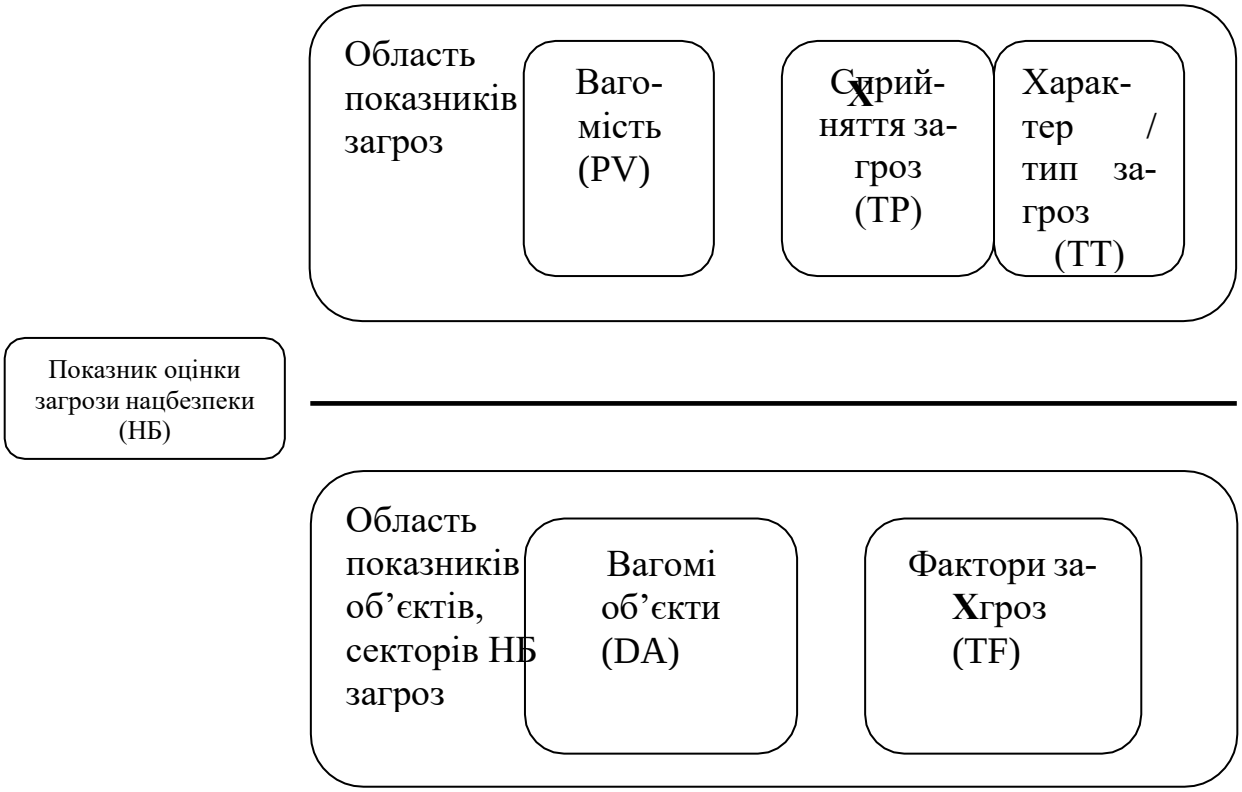

Рис. 2. Блок-схема – показник оцінки загрози національній безпеці в умовах цифровізації

Джерело: авторська розробка

Оцінці загроз у сфері нацбезпеки присвячено чимало наукових розробок, що здебільшого об'єднані єдиним напрямом – оцінка загроз і розподіл зброї (Threat Evaluation and Weapon Assignment – TEWA, наприклад [6; 7; 8; 10; 11]). TEWA вважається найпоширенішою моделлю

оцінювання на основі байєсівських мереж (Bayesian networks) [там само], нечіткої логіки [8; 9; 11] та систем підтримки прийняття рішень [2–4; 7; 12].

TEWA-моделі, засновані на мережах «bayesian networks», дозволяють долати невизначеності (неповнота інформації про об'єкти; відсутність інформації про стан інфраструктури; ймовірність та/або випадковість в управлінні конкретним озброєнням тощо) при моделюванні. У підході «bayesian networks» змінні TEWA-моделі містять межі ймовірностей або розподіл ймовірностей, що дозволяє оцінювати загрози навіть у разі неповноти даних.

У свою чергу, моделі, засновані на правилах концепції нечітких множин будуються за принципом функцій належності. У теорії поля та чітких множин члени x універсальної множини *X* є або членами, або не членами множини A ⊆ X.

Застосування систем прийняття рішень у TEWA-моделях дозволяє враховувати показники геоінформаційних систем (ГІС картрування вразливих активів), доповнювати модель методами прогнозування, розподіляти та оцінювати «економічно ефективне призначення зброї» [7]. Відтак, система прийняття рішень дозволяє розширити перелік параметрів моделі, а також оцінювати додаткові фактори (наприклад, економічну доцільність) при оцінці загроз. Самі TEWA-моделі із системою прийняття рішень можуть будуватися на основі машинного навчання (найпопулярніші моделі з древом рішень (цілей); більш просунуті моделі ґрунтуються на глибокому навчанні, наприклад Tactical Air Combat Decision Support System), теорії ігор, теорії поля та динамічних мереж («bayesian networks»).

Оцінка загроз найчастіше представлена двома [11] або трьома [7] етапами. Двоетапна модель передбачає таке: 1) оцінку та ранжування загроз; 2) призначення зброї. Триетапна модель складається з такого: 1) оцінки сприйняття загрози; 2) розрахунку індексу загроз (-и); 3) оцінка впровадження цифрових технологій у військовій сфері. Кожна модель оцінювання загроз нацбезпеці має право на існування. Кожен етап включає розрахунок конкретних характеристик [там само]. Так, на етапі сприйняття загрози розраховуються критичні параметри конкретного типу озброєння, що передбачає використання цифрових технологій (наприклад, крилатої ракети): швидкість, висота, поперечний перетин радіолокації / ефективна поверхня розсіювання радіолокаційних хвиль, маневреність, кут пікірування, атакуючий підхід та ін. Етап призначення зброї безпосередньо враховуючи характеристики наявного оборонного озброєння і містить параметри: а) загроза призначається зброї на основі індексу загрози; б) загроза з найвищим індексом загрози (TI).

Отже, узагальнено модель TEWA у сфері публічного управління рнацбезпекою в умовах впливу цифровізації та її технологій представляє собою оцінку та ранжування загроз у сфері безпеки за перерахованими вище

характеристиками, а також розрахунок відповідності оціненої загрози об’єктам/активам, що захищаються, із подальшим визначенням озброєння для забезпечення безпеки об’єктів та нейтралізації загроз. Безпосередньо оцінку загроз нацбезпеки (без розподілу озброєння) можна представити у вигляді блок-схеми (див. рис. 2), де розраховується загальна кількість загроз (при оцінці та ранжируванні) і виводиться показник відповідності загрози об'єкту/активу у сфері нацбезпеки, що захищається з боку держави.

Висновки. Оцінювання моделі публічного управління у сфері нацбезпеки в умовах впливу цифрових технологій запропоновано зреалізовувати шляхом аналізу стратегій та інших нормативно-правових актів у цій сфері, а також за станом функціонування освітньої та наукової сфер. Вони охоплюють кількість патентів у сфері розвитку цифрових технологій загалом і штучного інтелекту зокрема, стан надання «актуальних» знань у сфері цифровізації тощо. При цьому використано TEWA-модель. Власне, для цілей дослідження оцінено показники сприйняття загроз (ТР) та характеристика/тип загроз (ТТ), що концептуалізовані в такий спосіб сприйняття загрози у сфері нацбезпеки в умовах впливу цифровізації та її технологій:

1. Показник освіти.
2. Показник нормативно-правового регулювання.
3. Показник внутрішніх патентів.

Акцентовано, що практично всі звіти та дослідження мають «доктринальний» характер, а саме: вказують, що є якийсь тип загроз, пов’язаних із розвитком цифрових технологій і штучним інтелектом, що має певну характеристику загроз. Проте жодного їх статистичного чи математичного вираження немає. З огляду на це доцільно приймати рішення про побудову чисельного бінарного показника моделі впровадження публічного управління у сфері нацбезпеки в умовах впливу цифровізації та її технологій: 0 – тип/характер загрози відсутній у країні у звітному році; 1 – тип/характер загроз був присутній (зафіксований/ задокументований) у країні у звітному році згідно з наступним переліком типів/характеру загроз, пов’язаних з розвитком цифрових технологій і штучного інтелекту. Це загрози критичній інфраструктурі, кіберзагрози / кібератаки за допомогою штучного інтелекту, функціонуючі підприємства з дезінформації (зокрема Deepfakes), порушення прав людини (мається на увазі порушення персональних даних, загрози біометричним даним тощо).

Список використаних джерел:

1. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі: монографія. Харків: НУЦЗУ, 2024. 244 с.

2. Помаза-Пономаренко А.Л., Тарадуда Д.В. Кібербезпека об’єктів критичної інфраструктури: ґенеза координації дій складових сектору безпеки й

оборони // Матеріали Міжвідомчої науково-практичної конференції «Посилення спроможностей СБ України та взаємодія зі складовими сектору безпеки і оборони (27.09.2024, м. Київ).

3. Помаза-Пономаренко А.Л., Тарадуда Д.В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). https://www.inter-nauka.com/issues/administration2024/3/9732.

4. Помаза-Пономаренко А.Л., Тарадуда Д.В. Роль технологій цифровізації в ідентифікації об'єктів підвищеної небезпеки в контексті забезпечення цивільної безпеки // Матеріали III Всеукраїнської науково-теоретичної конференції «Держава і суспільство: сучасні виклики та пошук рішень» (16.05.2024, м. Київ). С. 337–340.

5. Тайер А.А. Вплив комунікативних технологій на ефективність публічного управління в Україні в умовах воєнного стану. URL: https://maup.com.ua/assets/files/dis/25-00-05/tajer-disertaciya.pdf/.

6. Cocelli M., Arkin E. A threat evaluation model for small-scale naval platforms with limited capability // EEE Symposium Series on Computational Intelligence. 2017. P. 1–8.

7. Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future directions / A. Naseem [et al.] // Annual Reviews in Control. 2017. Vol. 43. P. 169–187.

8. Johansson F., Falkman G. Comparison between two approaches to threat evaluation in an air defense scenario // Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). 2008. Vol. 5285. P. 110–121.

9. Galindo-Martin M.-A., Castano-Martinez M.-S., Mendez-Picazo M.-T. Digital Transformation, Digital Dividends and Entrepreneurship: A Quantitative Analysis // Journal of Business Research. 2019. Vol. 101(C), no. 146. P. 522–527.

10. Kumar S., Tripathi B. Modelling of Threat Evaluation for Dynamic Targets Using Bayesian Network Approach // Procedia Technology. 2016. Vol. 24. P. 1268–1275.

11. Naeem H., Masood A. An optimal dynamic threat evaluation and weapon scheduling technique // Knowledge- Based Systems. 2010. Vol. 23, Vol. 1. P. 337–342.

12. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Volume 14. Issue 1. Pp. 216–220. URL: https://www.magnanimitas.cz/ADALTA/140139/papers/K_10.pdf.

References:

1. Dombrovska S.M., Pomaza-Ponomarenko A.L., Kryukov O.I., Poroka S.G. Information threats and communication infrastructure in the public sector: a

monograph. Kharkiv: NUZZU, 2024. 244 p.

2. Pomaza-Ponomarenko A.L., Taraduda D.V. Cybersecurity of critical infrastructure objects: the genesis of coordination of actions of the components of the security and defense sector // Proceedings of the Interdepartmental scientific and practical conference "Strengthening the capabilities of the Security Service of Ukraine and interaction with the components of the security and defense sector (September 27, 2024, Kyiv).

3. Pomaza-Ponomarenko A.L., Taraduda D.V. Mechanisms for ensuring civil security of Ukraine: aspects of emergency prevention at the facilities of the military-industrial complex // Public administration and national security. 2024. No. 3 (44). https://www.inter-nauka.com/issues/administration2024/3/9732.

4. Pomaza-Ponomarenko A.L., Taraduda D.V. The role of digitization technologies in the identification of high-risk objects in the context of civil security // Proceedings of the 3rd All-Ukrainian scientific and theoretical conference "State and society: modern challenges and the search for solutions" (May 16, 2024, Kyiv). P. 337–340.

5. Thayer A.A. The influence of communication technologies on the effectiveness of public administration in Ukraine under martial law. URL: https://maup.com.ua/assets/files/dis/25-00-05/tajer-disertaciya.pdf/.

6. Cocelli M., Arkin E. A threat evaluation model for small-scale naval platforms with limited capability // EEE Symposium Series on Computational Intelligence. 2017. P. 1–8.

7. Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future directions / A. Naseem [et al.] // Annual Reviews in Control. 2017. Vol. 43. P. 169–187.

8. Johansson F., Falkman G. Comparison between two approaches to threat evaluation in an air defense scenario // Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics). 2008. Vol. 5285. P. 110–121.

9. Galindo-Martin M.-A., Castano-Martinez M.-S., Mendez-Picazo M.-T. Digital Transformation, Digital Dividends and Entrepreneurship: A Quantitative Analysis // Journal of Business Research. 2019. Vol. 101(C), no. 146. P. 522–527.

10. Kumar S., Tripathi B. Modelling of Threat Evaluation for Dynamic Targets Using Bayesian Network Approach // Procedia Technology. 2016. Vol. 24. P. 1268–1275.

11. Naeem H., Masood A. An optimal dynamic threat evaluation and weapon scheduling technique // Knowledge- Based Systems. 2010. Vol. 23, Vol. 1. P. 337–342.

12. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Volume 14. Issue 1. Pp. 216–220. URL: https://www.magnanimitas.cz/ADALTA/140139/papers/K_10.pdf.